IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

K.MIZRA, LLC,	)	
	)	
Plaintiff,	)	**C.A. NO. 6:20-CV-01031-ADA**
	)	
v.	)	
	)	[redacted]
CISCO SYSTEMS, INC.	)	
	)	
Defendant.	)	
	)	

DEFENDANT CISCO SYSTEMS, INC.'S REPLY BRIEF IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT OF NONINFRINGEMENT

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. UNDISPUTED FACTS 2

III. ARGUMENT 4

A. Cisco does not sell, and there is no proof that Cisco has ever assembled or used, the Accused Combination of Cisco and non-Cisco products 4

B. Even assuming assembly and use, K.Mizra has identified no triable issues on the missing TPM or DNS limitations.....8

IV. CONCLUSION.....10

TABLE OF AUTHORITIES

Page(s)

Cases

ACCO Brands, Inc. v. ABA Locks Mfr. Co.,
501 F.3d 1307 (Fed. Cir. 2007).....8

Ball Aerosol & Specialty Container, Inc. v. Limited Brands, Inc.,
555 F.3d 984 (Fed. Cir. 2009).....8

Centillion Data Systems, LLC v. Qwest Commc'ns Int'l, Inc.,
631 F.3d 1279 (Fed. Cir. 2011).....6

Cross Medical Products, Inc. v. Medtronic Sofamor Danek, Inc.,
424 F.3d 1293 (Fed. Cir. 2005).....6

Deep9 Corp. v. Barnes & Noble, Inc.,
No. C11-0035JLR, 2012 WL 4336726 (W.D. Wash. Sept. 21, 2012), *aff'd*,
504 F. App'x 923 (Fed. Cir. 2013) (unpub.).....8

Deepsouth Packing Co. v. Laitram Corp.,
406 U.S. 518 (1972).....1, 5

E-Pass Tech., Inc. v. 3Com Corp.,
473 F.3d 1213 (Fed. Cir. 2007).....4

Ericsson, Inc. v. D-Link Sys., Inc.,
773 F.3d 1201 (Fed. Cir. 2014).....6

Estech Systems, Inc., v. Howard Midstream Energy Partners,
No. 6:20-CV-777-ADA, ECF No. 131 (W.D. Tex. Aug. 31, 2022).....4

ESW Holdings, Inc. v. Roku, Inc.,
No. 6-19-CV-00044-ADA, 2021 WL 1069047 (W.D. Tex. Mar. 18, 2021).....4, 5

INVT SPE LLC v. ITC,
46 F.4th 1361 (Fed. Cir. 2022) 1, 7, 8

LifeNet Health v. LifeCell Corp.,
837 F.3d 1316 (Fed. Cir. 2016).....6

Rotec Indus., Inc. v. Mitsubishi Corp.,
215 F.3d 1246 (Fed. Cir. 2000).....5

SiRF Tech., Inc. v. ITC,
601 F.3d 1319 (Fed. Cir. 2010).....6

The Massachusetts Inst. of Tech. v. Abacus Software, Inc.,
No. 5:01–CV344, 2004 WL 5268128 (E.D. Tex. Aug. 24, 2004).....1

Statutes

35 U.S.C. § 271(a) 1, 4

I. INTRODUCTION

K.Mizra's infringement theories have become ever more implausible. It has abandoned indirect infringement; the sole remaining claim is that Cisco literally, directly infringes five claims of the '705 Patent. ECF No. 139, "Opp." at 6. As K.Mizra has it, Cisco is liable for direct infringement even though "Cisco itself does not sell" the complete claimed system configured as the claims require, Opp. at 7, and there is no evidence that Cisco or any Cisco customer has ever assembled or used that complete system. That sounds wrong because it is wrong.

Based on the statutory language and longstanding precedent, direct infringement requires making, using, or selling the complete "patented invention." 35 U.S.C. § 271(a); *see also, e.g.*, *The Massachusetts Inst. of Tech. v. Abacus Software, Inc.*, No. 5:01–CV344, 2004 WL 5268128, at *19–20 (E.D. Tex. Aug. 24, 2004) (in enacting § 271(f) Congress "did not amend § 271(a) or otherwise modify the rationale" of the seminal case interpreting § 271(a), *Deepsouth Packing Co. v. Laitram Corp.*, 406 U.S. 518, 526–29 (1972)). That K.Mizra's theory requires multiple Cisco and non-Cisco products is fatal.

K.Mizra denies that it bases its claim on mere capability to infringe. Opp. at 5. But even when a software claim is read to require only the capability of performing recited functions, the Federal Circuit has "never suggested that reasonable capability can be established without any evidence or undisputed knowledge ***of an instance*** that the accused product performs the claimed function when placed in operation." *INVT SPE LLC v. ITC*, 46 F.4th 1361, 1376 (Fed. Cir. 2022) (emphasis added). K.Mizra has no evidence of any such instance. Not even one.

Its theories are also a moving target. In moving to exclude Cisco's damages expert, K.Mizra explained that it "accuses certain Cisco ISE and AnyConnect products ("Accused Products") running on Windows 10 or 11." ECF No. 130 at 1. In opposing Cisco's motion to exclude its damages expert, K.Mizra acknowledged that "[t]he Accused Products are software with

subscription level licenses." ECF No. 146 at 15. That opposition was filed the same day as this one. But here, K.Mizra, perhaps recognizing that its concessions preclude infringement of the system claims for lack of a processor sold by Cisco, says that Cisco hardware (the Cisco Secure Network Server) is required too. Opp. at 4–5. K.Mizra should be bound by its concessions that it accuses a combination of Cisco software products. But whether or not Cisco hardware is required too, K.Mizra has no proof that Cisco or anyone has ever assembled or used the accused system with all of the components, configurations, instructions, and hardware required to allegedly infringe. This is a fundamental and fatal deficiency. There is not enough here to get to a jury.

K.Mizra also cannot prove that any Cisco product is associated with a TPM, nor is there any evidence that Cisco products are even capable of employing DNS redirection to perform quarantining, as every claim requires. Each of these additional problems is independently fatal.

II. UNDISPUTED FACTS

K.Mizra does not answer Cisco's undisputed facts, falsely asserting that Cisco cited no evidence. Opp. at 2. Cisco cited extensive evidence, including many concessions by K.Mizra's experts. *See* ECF No. 119, "Mot." at 1–5. At least the following facts are beyond dispute:

- K.Mizra now defines the "Accused System" as ISE "as sold and employed in conjunction with the Cisco 'AnyConnect' Secure Mobility Client and the Cisco Secure Network Server," and alleges that Cisco directly infringes claims 12 and 19 because "the two Cisco products (ISE and AnyConnect) interact and 'talk to each other' over a computer network." Opp. at 3.
- To possess the accused posture check feature, ISE and AnyConnect must be deployed together at the highest, or "Premier" license levels; someone must select certain settings, and the computer(s) running AnyConnect must have Windows 10 or 11, which Cisco doesn't sell or require. Mot. at 3 (citing Ex. E at 25:16–20, 26:19–25, 27:14–28:19).

- ISE and AnyConnect at the Premier license level are sold separately; each can be used without the other; and they can be used together for purposes other than the accused posture check. Mot. at 3–5, 13 (citing evidence including Ex. I (ISE Guide) at 20, 26, 33–35 (which Dr. Cole considered, Ex. C No. 464)); Opp. at 6 (declining to respond to pages 12–24).
- Although K.Mizra says ISE "is" sold with Cisco's SNS hardware product, the cited testimony confirms [redacted]. Opp. at 3 (citing Ex. C (Nygaard Dep. Tr.) at 30:17–31:23).
- The Cisco products, as sold, are not configured with the policy, containment or redirection settings K.Mizra's theory requires. K.Mizra's expert conceded that it is the customer who configures settings, including redirection settings, and determines the posture-check policies. Not Cisco. Mot. at 3 (citing Ex. E at 25:16–20, 26:19–25, 27:14–28:19).
- There is no evidence of testing by Cisco anywhere, let alone in the United States. Its expert testified that Cisco does not put the products into use. *Id.* at 6 (citing Ex. E at 29:1–37:4).
- K.Mizra has no evidence that the accused products have been combined, configured, or used by anyone in the manner it claims infringes. *See* Mot. at 8–9 (K.Mizra's expert's admissions).
- Cisco ISE and AnyConnect do not even allegedly contain a TPM. K.Mizra assumes that some customers install AnyConnect on their own computers, some of which run Windows 10/11, and that such computers have TPMs. Mot. at 4–5 (citing Ex. F at 31, 32–42; Ex. E at 43:17–44:7). Cisco does not make, direct, or require these customer choices. Mot. at 6.
- There is no evidence that AnyConnect calls anything other than Microsoft API routines, or that AnyConnect or the Microsoft APIs actually calls a TPM. Mot. at 14 (citing evidence).
- There is no evidence that the Cisco products ever return the IP address of a quarantine server in response to a DNS query. Mot. at 10–11, 16; Opp. at 10–11.

III. ARGUMENT

A. Cisco does not sell, and there is no proof that Cisco has ever assembled or used, the Accused Combination of Cisco and non-Cisco products.

K.Mizra's direct infringement theories for all claims fail as a matter of law. K.Mizra can prevail only by showing that Cisco itself "makes, uses, offers to sell, or sells any patented invention, within the United States." 35 U.S.C. § 271(a). That is a hopeless task, because the infringement claim requires multiple Cisco and non-Cisco products, and K.Mizra has no evidence that Cisco (or anyone) has ever assembled this combination into the "patented invention."

Method Claim (Claim 1). K.Mizra effectively concedes it has no evidence that Cisco performs each step. *Compare* Mot. at 5–7 (showing lack of evidence) *with* Opp. at 5 (offering no substantive response). K.Mizra's appeal to "circumstantial evidence" is a red herring, because K.Mizra doesn't cite ***any*** evidence, circumstantial or not, that Cisco ever performed the claimed steps. Speculation about supposed "internal testing" is not evidence. *Id.* Particularly given its unrebutted expert concessions, *supra* at 2–3, K.Mizra has no proof concerning the method claim.

None of K.Mizra's cited cases suggests that the Court can infer without evidence that Cisco practices each step—that is contrary to black-letter law. *See, e.g., E-Pass Tech., Inc. v. 3Com Corp.*, 473 F.3d 1213, 1222 (Fed. Cir. 2007) (refusing to make "speculative leap," without evidence, any customers "actually performed the claimed method"); *ESW Holdings, Inc. v. Roku, Inc.*, No. 6-19-CV-00044-ADA, 2021 WL 1069047, at *2 (W.D. Tex. Mar. 18, 2021). As a matter of law, K.Mizra cannot prove infringement of this claim. *See, e.g.*, *Estech Systems, Inc., v. Howard Midstream Energy Partners,* No. 6:20-CV-777-ADA, ECF No. 131 at 13 (W.D. Tex. Aug. 31, 2022) (granting summary judgment absent evidence that any user actually performed required limitation).

System Claim (Claim 12). Claim 12 requires, among other things, a system with "a processor configured to" perform the method of claim 1. Cisco does not infringe Claim 12 because

it does not make or sell a system that meets all the limitations of Claim 12. Among other things, Cisco concededly does not make, use, or sell a host computer, an operating system running on a host computer, or a TPM. Opp. at 7 ("Cisco itself does not sell a TPM or host computer as part of the Accused System."). Not surprisingly, K.Mizra cites no authority for the proposition that a party that sells a partial system can directly infringe without evidence that it ever assembled the full system.[1] Nor is there any dispute that the Cisco products, as sold, lack the policy, containment, or redirection settings K.Mizra's infringement claim requires. *Supra* at 2–3.

K.Mizra conflates the question of whether the "Accused System" infringes with whether *Cisco* infringes. It asserts that its expert "demonstrates how each of the recited functions is performed by the *Accused System* and its processor." Opp. at 4 (emphasis added). Dr. Cole does no such thing, but even if he did, the "Accused System" is not synonymous with "Cisco." It includes multiple and separate Cisco products, which Dr. Cole's opinion requires ***customers*** to combine with non-Cisco products. *Supra* at 2–3.

It is axiomatic that making or selling components that might be combined into an invention is not direct infringement. *See Deepsouth*, 406 U.S. at 528 (§ 271(a) "protects only against the operable assembly of the whole, and not the manufacture of its parts"). "*Deepsouth* remains good law [regarding § 271(a)]: one may not be held liable for 'making' or 'selling' less than a complete invention." *Rotec Indus., Inc. v. Mitsubishi Corp.*, 215 F.3d 1246, 1252 n.2 (Fed. Cir. 2000); *see also ESW Holdings Inc. v. Roku Inc*., 2021 WL 1069047, at * 5 (granting summary judgment where

[1] K.Mizra ignores this fundamental rule again in its brief discussion of dependent claims 9 and 16, which add that "the software component on the first host is an operating system." The "operating system" K.Mizra accuses is Windows. Opp. at 6. K.Mizra has no evidence of Cisco testing or use with Windows, much less in the United States. Cisco did not separately move for summary judgment on these claims, which fall along with the independent claims. But K.Mizra's argument shows that it cannot establish infringement of the dependent claims as a matter of law.

defendant lacked "control over each component").

K.Mizra tries to avoid this outcome by asserting that the third-party components only perform "unclaimed actions." Opp. at 7. That does not answer the fundamental problem that K.Mizra's theory requires two different *Cisco* products to be combined and configured, and to "talk to" each other. Opp. at 3. And the TPM and host computer are both claim limitations. K.Mizra's effort to minimize the TPM as "unclaimed" is indefensible given that the applicant added the TPM limitation during prosecution expressly to avoid anticipation. *See* Ex. J, ECF No. 119-11, at -2968–73, -3011–12, -3082–84 (applicant's argument that prior art did not teach TPM).

The cases K.Mizra cites do not help its cause. *LifeNet Health v. LifeCell Corp*., 837 F.3d 1316 (Fed. Cir. 2016) fully supports Cisco's position. There, all limitations were "met without action by a third party." *Id.* at 1326. *LifeNet* itself distinguishes its facts from cases directly analogous to this one, where no infringement was found. *Id.*; *see Cross Medical Products, Inc. v. Medtronic Sofamor Danek, Inc.*, 424 F.3d 1293, 1311–12 (Fed. Cir. 2005) (manufacturer of surgical implants did not directly infringe where implants had to be "operatively joined" to bone segment by third-party surgeon); *Centillion Data Systems, LLC v. Qwest Commc'ns Int'l, Inc.*, 631 F.3d 1279, 1288 (Fed. Cir. 2011) (accused infringer who provided software did not practice limitation requiring "personal computer data processing means" where customers decided to install and operate the software on computer). As for *SiRF Tech., Inc. v. ITC*, 601 F.3d 1319, 1329–31 (Fed. Cir. 2010), there, the manufacturer performed the claimed steps, which Cisco does not, and SiRF's customers could not modify its system. "*SiRF* did not create direct infringement liability whenever an alleged infringer sells a product that is capable of executing the infringing method." *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1221–22 (Fed. Cir. 2014).

Computer program product claim (Claim 19). Claim 19 requires "[a] computer program

product … embodied in a non-transitory computer readable medium and comprising computer instructions for" performing the method of claim 1. K.Mizra's mix-and-match infringement theory also fails here. It has not identified any Cisco product that is "programmed or otherwise configured, ***without modification***, to perform the claimed function when in operation." *INVT*, 46 F.4th at 1376 (emphasis added). To start with the facts: K.Mizra tries to elide its multiproduct, customer-driven theory, by simultaneously acknowledging that ISE and AnyConnect are separate Cisco products that users may use together, and baldly asserting that Dr. Cole "has shown ISE, as provided by Cisco, meets all limitations of claim 19 in a customer environment." Opp. at 3–4. Saying that doesn't make it so. He does not show that ISE by itself embodies all limitations; rather, his opinion lumps together products that a Cisco user may choose to use together, but are "completely separate," Opp. Ex. C, ECF No. 139-3, at 8–9, and depends upon customer-selected configuration, settings, and deployment on Microsoft 10/11 computers. *Supra* at 2–3.

As with claim 12, K.Mizra has an insuperable *Deepsouth* problem. K.Mizra has not identified any Cisco "computer program product" that is "embodied in a nontransitory computer readable medium" and "comprising instructions for" the entire method. Rather, it alleges that "ISE and AnyConnect" ***together*** provide instructions; that AnyConnect further "interfaces" with Windows; and that Windows requires a TPM. *See* Opp. at 4, 8. Dr. Cole tries to show infringement of Claim 19 based ***solely*** on his analysis of claim 1 (Opp. Ex. B, ECF No. 139-2, at 139–42)—which requires the interactions of multiple products, Cisco and non-Cisco. Nowhere does K.Mizra identify a single computer program product with the instructions. Under *Deepsouth*, K.Mizra loses.

K.Mizra ignores Cisco's unrebutted evidence that customers, not Cisco, must make the modifications (including installing AnyConnect on Windows 10/11 devices) and choose the settings that K.Mizra accuses. K.Mizra indisputably has no evidence that the policy, containment,

or remediation settings required by the claims are required or default settings of ISE as sold. K.Mizra ignores *INVT*, 46 F.4th at 1376, *Ball Aerosol & Specialty Container, Inc. v. Limited Brands, Inc.*, 555 F.3d 984, 994–95 (Fed. Cir. 2009), and *ACCO Brands, Inc. v. ABA Locks Mfr. Co.*, 501 F.3d 1307, 1313 (Fed. Cir. 2007), which confirm that K.Mizra cannot show infringement based on customers' choices. The customer-supplied settings and Windows 10/11 preclude infringement. *See also, e.g., Deep9 Corp. v. Barnes & Noble, Inc.*, No. C11-0035JLR, 2012 WL 4336726, at *13–14 (W.D. Wash. Sept. 21, 2012) (no infringement of Beauregard claim, because defendant "did not provide . . . the Internet"), *aff'd*, 504 F. App'x 923 (Fed. Cir. 2013) (unpub.).

K.Mizra also has no evidence that anyone has ever combined the accused products in the manner it claims infringes. It ignores, and does not rebut, its expert's admissions. Mot. at 8, 9. It falsely asserts (Opp. at 10) that Cisco's expert admitted AnyConnect is installed on Windows 11 machines, but Dr. Clark did not say that. *See* Opp. Ex. E, ECF No. 139-5 at 103:1–15. Even if claim 19 were read to require mere capability, K.Mizra still has not shown a triable issue. As the Federal Circuit explained in *INVT*: "Because we require claim limitations to have some teeth and meaning, proof of reasonable capability of performing claimed functions requires, at least as a general matter, proof that an accused product—when put into operation—*in fact executes all of the claimed functions at least some of the time or at least once in the claim-required environment*." 46 F.4th at 1377, 1380 (emphasis added). Even if a customer buys the multiple products needed and puts them together, there is no evidence of *any* instance of Cisco or a customer choosing the claimed policy, containment, or redirect settings, or using a host device that contains a TPM.

B. Even assuming assembly and use, K.Mizra has identified no triable issues on the missing TPM or DNS limitations.

There are no triable issues regarding TPM or DNS. These are not "unclaimed limitations."

Trusted Platform Module. K.Mizra acknowledges that "the infringing product … must

interact with a trusted platform module." Opp. at 6. There is no evidence that Cisco's ISE or AnyConnect products ever do so.[2] There is certainly no evidence that comes close to satisfying the high bar K.Mizra's invalidity expert set for this limitation.

K.Mizra invokes speculative and conclusory assertions that, when installed on a Windows 10/11 device, certain Microsoft routines use random numbers generated by the TPM. Opp. at 3, 8–10 (arguing that Dr. Cole cited [redacted] Ex. E, ECF No. 119-6 at 132:21–135:4, 135:11–15, 136:15–140:20. None of this shows that AnyConnect or the Microsoft APIs calls a TPM. Microsoft source code would be required for that, and K.Mizra has none. It suggests source code may not be required. Opp. at 3. But the claims require ***association with*** the TPM. Dr. Cole recognized that code determines functionality, and that no Microsoft source code or documentation shows his cited routines calling a TPM. Mot. at 14. K.Mizra also does not dispute that Dr. Cole failed to explain how AnyConnect uses this random number, and ***nowhere*** asserts that the accused posture feature does so. *Id.*

In addition, the undisputed evidence shows that K.Mizra cannot maintain its infringement claim without violating the fundamental rule against twisting the patent one way to avoid invalidity and another to show infringement. K.Mizra asserts that Cisco has not shown how the TPM-related opinions of its experts conflict. Opp. at 7. Yes, Cisco has. Cisco explained K.Mizra's infringement theory with record cites. Mot. at 14–15. Its opposition confirms that its infringement theory of association with the TPM is, to put it charitably, "high-level." Opp. at 8–10. Cisco explained how

[2] K.Mizra mischaracterizes Dr. Clark's testimony. Opp. at 10. [redacted] Opp. Ex. E, ECF No. 139-5, at 103:16–21.

K.Mizra's validity expert advances a different, higher threshold of what the TPM must do to meet the claim language. Mot. at 15 (citing validity expert report and testimony). K.Mizra's opposition confirms that its experts read the TPM limitation inconsistently: it makes no attempt to show that Cisco uses a cleanliness attestation generated by a TPM, or that the TPM played any role in generating the keys used to sign it. The scope K.Mizra's validity expert applied is thus an additional barrier to infringement.

DNS. Cisco used "DNS redirect" as shorthand for the full limitation of every asserted claim that requires quarantining the computer attempting network access in a specific way: by returning the IP address of the quarantine server instead of the IP address for the requested URL. Mot. at 15 & n.13. K.Mizra has no evidence of this limitation. It fails to answer Cisco's points, instead contending that Cisco's ISE witness testified that Cisco uses DNS *queries* widely. Opp. at 10–11 (quoting Ex. C (Nygaard Dep. Tr.) at 94:4–15). That does not create a triable issue of fact. It says nothing about what IP address ISE ***returns*** in response to any given DNS query. And even if it established that Cisco ISE widely uses DNS ***redirection*** (that is, returning a different IP address than the one requested), given the undisputed evidence, that would not permit a reasonable juror to conclude that Cisco uses DNS redirection in the claimed manner, to return the address of a quarantine server. There is no evidence of that. K.Mizra does not refute that its expert identified something completely different (URL or HTTP redirection)[3] and conceded [redacted] Mot. at 16 (citing Ex. F at 68, 71, 73; Ex. E at 200:23–202:23, 199:20–200:5 (URL redirect shown in report; could not recall seeing DNS redirect in the code)).

IV. CONCLUSION

K.Mizra has failed to demonstrate facts on which a reasonable jury could find infringement.

[3] K.Mizra also implicitly concedes what its validity expert acknowledged and the prosecution history makes clear: DNS redirection and URL/HTTP redirection are distinct. Mot. at 16.

Dated: June 30, 2023

Respectfully submitted,

By: */s/ Melissa R. Smith*

Melissa R. Smith (State Bar No. 24001351)
melissa@gillamsmithlaw.com
GILLAM & SMITH LLP
303 South Washington Avenue
Marshall, TX 75670
Telephone: (903) 934-8450
Facsimile: (903) 934-9257

Elizabeth R. Brannen (*Pro Hac Vice*)
ebrannen@stris.com
Kenneth J. Halpern (*Pro Hac Vice*)
khalpern@stris.com
Sarah Rahimi *(Pro Hac Vice)*
srahimi@stris.com
STRIS & MAHER LLP
777 S. Figueroa St, Ste 3850
Los Angeles, CA 90017
Telephone: (213) 995-6800
Facsimile: (213) 216-0299

Jhaniel James *(Pro Hac Vice)*
jjames@stris.com
STRIS & MAHER LLP
111 N Calhoun St, Ste 10
Tallahassee, FL 32301
Telephone: (213) 995-6800
Facsimile: (813) 330-3176

Attorneys for Defendant
Cisco Systems, Inc.

CERTIFICATE OF SERVICE

I certify that on June 30, 2023, the documents filed with the Clerk of Court via the Court's CM/ECF system under seal in the above-captioned case were subsequently served on all counsel of record by electronic mail.

/s/ Melissa R. Smith
Melissa R. Smith